# 5 FAM 750
# ELECTRONIC MAIL (EMAIL) POLICY

*(CT:IM-122;  11-14-2011)*
*(Office of Origin:  IRM/OPS/MSO/EML)*

## 5 FAM 751  EMAIL

### 5 FAM 751.1  PURPOSE

*(CT:IM-122;  11-14-2011)*

This policy explains the email services the Bureau of Information Resource Management (IRM) provides, as well as the actions Department personnel should take to manage their email accounts.

### 5 FAM 751.2  SCOPE

*(CT:IM-122;  11-14-2011)*

a. Establishes policy which applies to the email management operations of Microsoft Outlook.

b. Defines policies with respect to mailbox limits, prohibitions when using email, email etiquette, management, and markings.

c. This policy applies to OpenNet and ClassNet email accounts both domestically and abroad.

### 5 FAM 751.3  AUTHORITIES

*(CT:IM-122;  11-14-2011)*

a. Privacy Act of 1974, as amended (5 U.S.C. 552(a)).

b. Freedom of Information Act (FOIA) of 1966, as amended; privacy exemptions (5 U.S.C. 552(b)6 and (b)7(c)).

c. Paperwork Reduction Act (PRA) of 1995 (44 U.S.C. 3501 et seq.).

d. E-Government Act of 2002, Section 208 (44 U.S.C. 3602).

e. Safeguarding Against and Responding to the Breach of Personally Identifiable Information, M-07-16 (May 22, 2007).

f. 36 CFR Parts 1220, 1222, 1228, and1234 Electronic Mail Systems August 28, 1995.

g. Executive Order 13526, Classified National Security Information

h. The authorities found in 1 FAM 271.5 and 5 FAM 113.

i. The Federal Records Act (44 U.S.C. 31).

# 5 FAM 752 USING THE EMAIL SYSTEM

*(CT:IM-122; 11-14-2011)*

a. IRM determines the limit of each user's mailbox, based on technology and available hardware. The limit does NOT include Microsoft personal folders, which are stored in .pst files on a network drive rather than on an Exchange server. Email attachments are subject to size and type restrictions according to policy. Attachments larger than 30 MB are prohibited and will not be delivered.

b. When a user's mailbox reaches its limit, IRM works with the user to apply best practices/email tips to reduce the mailbox size, and/or create personal folders and help move mailbox items to the .pst file. To ensure this is done in a timely manner, IRM reserves the right to create .pst files and move items to them on behalf of the user. This is necessary in cases when the user is out of the office on leave/travel or delays taking action to reduce the .pst file size. Should this become necessary, IRM records the location of the personal folder and ensures the user is notified of the change.

c. The IRM Email Review Board reviews requests for exceptions to the mailbox storage limit. Guidance on exceptions, including how to request increased mailbox size, is available at the Email Mailbox Management Web site on the "Request Procedure" tab.

## 5 FAM 752.1 Prohibitions When Using Email

*(CT:IM-122; 11-14-2011)*

a. Limited personal use of email via U.S. Government computer systems is authorized as described in 5 FAM 723, Personal Use of U.S. Government Equipment.

b. Do not send electronic greetings (e-cards); non business-related multimedia files; chain letters; letters or messages that offer a product or service based on or tied to a chain letter structure, including jokes, recipes or other non-business-related information; conduct any other activity that congests or disrupts the Intranet or Internet.

c. Never use "Reply to all" unless the response is applicable to all addressees. Only send "reply" email to those parties to whom action or pertinent information is directed. The over-use of "Reply to All" email

responses slows down messaging for all users and regularly creates backlogs in users' inboxes.

d. Unclassified material, including Sensitive But Unclassified (SBU), may be transmitted in email on the Internet. However, in accordance with 12 FAM 544.3, individual employees should decide whether or not unencrypted email provides adequate protection for the specific information they are transmitting. For example, if the email contains a significant amount of sensitive personally identifiable information (PII) (e.g., a list of social security and/or credit card numbers), the sender should consider using an encrypted or other more secure means of transmission, so it does not place that information at a high risk of possible compromise. In accordance with 5 FAM 469 and 12 FAM 544, employees should understand their responsibilities for protecting PII to which they have authorized access in performance of their official duties. Prior to sending emails that contain PII, employees should consider the risk associated with the transmission and use approved Department technology to properly secure the data during transmission. Posting or discussing classified or SBU information on any Web site, chat room, or other public forum on the Internet is strictly prohibited (see 5 FAM 731 paragraph h).

e. To preclude inadvertent transmission of inappropriate information on the Internet, the "Auto Forward" capability must not be used to send Department emails to an Internet address. Additionally, users must never put their personal email address in any out-of-office correspondence.

f. Use of email services on U.S. Government computers is subject to monitoring as described in 5 FAM 724, Monitoring and Auditing Policies. Where warranted, systems personnel must give any actual or potential evidence of criminal activity involving Department computers to law enforcement and other authorized security officials.

g. The Department reserves the right to access all messages sent or received on its electronic mail systems. Systems managers, systems administrators, records managers, and security officials may monitor, or audit with appropriate managerial approvals as provided for in 5 FAM 724, the system to ensure that all electronic mail transactions comply with applicable policies defined in 5 FAM 700 and 12 FAM 500 AND 12 FAM 600 series.

# 5 FAM 753 MARKING EMAIL

## 753.1 Classification and Sensitivity Markings

*(CT:IM-122;  11-14-2011)*

a. Classified emails must be marked in accordance with E.O.13526. Limited distribution email should include marking in accordance with requirements in 5 FAH-2 H-440 Captions and Handling Instructions and 5 FAM 460 The Privacy Act and Personally Identifiable information.

b. SMART provides an automated tool to mark and correctly place drafter-provided classification and sensitivity designators in the header and metadata fields of the email. The drafter must manually format the portion markings for classified messages, especially portion marking each subject line, headers, and paragraphs.

## 753.2 Administrative Markings

*(CT:IM-122;  11-14-2011)*

a. Employees must avoid giving the false impression they are acting in an official capacity when they are using U.S. Government office equipment for non-Government purposes (e.g., personal emails). If there is expectation that such personal use could be interpreted to represent an agency, then you must use an adequate disclaimer. An acceptable disclaimer is "The views expressed in this email are solely those of (sender), and in no way reflect the views of the U.S. Department of State or the U.S. Government." Employees should use the signature block to properly identify themselves.

b. On their Department email accounts, contractor personnel must use an email signature block that shows name, the office being supported, and company affiliation (e.g., "John Smith, Office of Human Resources, ACME Corporation Support Contractor").

# 5 FAM 754 EMAIL MANAGEMENT

*(CT:IM-122;  11-14-2011)*

a. Users are to actively manage their email accounts and avoid retaining unnecessary email in their mailbox.

b. Email originators and recipients are required to determine if an email is appropriate for preservation and, to the extent necessary, properly archive the email outside their email mailboxes. Placing an email in personal folders is NOT an adequate substitute for preserving the item as a record. SMART users who identify a working email that needs archiving should click the Convert to Archive button in Microsoft Outlook. This opens an archive message form that allows users to send the message to the Archive, where it is retained and available for SMART searches.

c. Working emails are NOT stored in the Archive, but they still require classification and sensitivity markings. Examples of working emails include:

- Messages documenting routine activities containing non substantive information, such as routine notifications of meetings, scheduling of work-related trips and visits, and other scheduling related activities.
- Messages containing drafts that do not provide understanding of the formulation and execution of basic policies, decisions, actions, or responsibilities.
- Messages containing quasi-official notices including memoranda and other records that do not serve as the basis of official actions, such as notices of holidays or charity and welfare fund appeals, bond campaigns, and similar records.
- Material retained for reference while working on a project that is no longer needed when the project is complete**,** provided the material does not warrant long-term preservation.
- Personal exchanges unrelated to official business.

d. As with other documentary materials, users must take steps to preserve emails where required by legal mandates (e.g., emails relevant to actual or anticipated litigation or in response to pending requests from Congress or under the Freedom of Information Act.) Email systems administrators must also take steps to preserve emails when authorized.

e. Email messages are records when they meet the definition of a record as stated in the Federal Records Act (44 U.S.C. 3301). Email messages are records when:

(1) An agency makes messages related to Federal law or in connection with public business; and

(2) There is information regarding Governments which provides informational value of the data.

f. Email message creators and recipients must decide whether a particular message is appropriate for preservation in the Archive. Consistent with 5 FAM 443, principal categories of materials, including email, that must be preserved are: records that document the formulation and execution of basic policies and decisions and the taking of necessary actions; records that document important meetings; records that facilitate agency officials' and their successors' action; records that make scrutiny by the Congress or other duly authorized agencies of the Government possible; and records that protect the financial, legal, and other rights of the Government and of persons directly affected by the Government's actions. See 5 FAM 443 and the Records Management website for Record email identification.

g. Record emails may contain memos, external correspondence, and other documents with long-term value. They may be approved and cleared, depending on the drafter, and may carry organizational authority. In SMART there are two types of record emails:

   (1) Directly addressed messages sent to one or more individuals; and

   (2) For-the-record messages sent directly to the Archive.

h. Users are to review 5 FAM 443, Electronic Mail (Email) Records, for further responsibilities for handling email correspondence.

i. Current guidelines on records management and archiving are found at Bureau of Administration website. Click on the Records Management link.

# 5 FAM 755 EMAIL ETIQUETTE

*(CT:IM-122; 11-14-2011)*

a. Record emails may be preserved permanently as part of the Department's historical record. As with all official transactions, employees should adhere to professional etiquette standards when drafting record emails.

b. Avoid mixing professional and personal information in a single email or thread when practicable. Also, remove all non-business-related content from a "for-the-record" message before sending it to the SMART Archive.

c. You should notify the original sender if you decide to convert a working email from another individual to a record email and apply the appropriate markings.

# 5 FAM 756 THROUGH 759 UNASSIGNED

*(CT:IM-122; 11-14-2011)*